

REMARKS

The Examiner rejected portions of the disclosure and the title. This amendment corrects those areas.

The new claims presented herein include more detail to distinguish the cited references. These new claims add no new matter.

The Examiners rejected claims 1, 3, 5, 11 and 13 under 35 112, second paragraph, citing indefiniteness. The new claims have been reviewed to ensure that these types of errors are not present.

The Examiner rejected claims 1, 3 and 13 under 35 USC 102(e) citing U.S. pat. no. 6,108,420 to Larose et al. (Larose). The remaining claims were rejected under 35 USC 103(a) using Larose as the primary reference and U.S. patents no. 6,240,513 to Friedman et al. (Friedman) and then U.S. pat. no 6,026,166 to LeBourgeois (LeBourgeois).

A new set of claims is presented in this amendment, but the Examiner's findings in the office action are instructive. On page 5, paragraph 13, the Examiner determined that "Larose is silent on the matter of encrypting the software product using the first value..." Later in the same paragraph the Examiner determined that "using keys that are derived from device/system parameters are commonly implemented in the art." The Examiner used Larose as anticipating the claims that did not have the computer parameters cited as a source of a key, and Larose and Friedman as suggesting the claims that had the computer parameters, and Larose, Friedman and Lebourgeois as suggesting the claims

containing a “quorum.” As a general comment (more detail follows) Larose and Friedman all *require* the use of PPK’s (Public/Private Keys). Larose explicitly states that usage of PPK is required to realize the advantages of his invention. Friedman is also reliant upon the creation and usage of PPK and LeBourgeois’s signatures are based on PPK’s, and the only reasonable way of combining them includes use of these PPK’s (whereas the present claims do not use PPK and are reliant upon different techniques). Furthermore, because all the cited patents are reliant upon PPK, they all require the sending of unencrypted public keys to the installation computer--a weakness partly acknowledged in Larose (see detailed discussion below) insofar as recognizing the issue of *storing* such unencrypted public keys on the installation computer. The present invention both recognizes and overcomes this, and other, problems inherent in the cited patents. Finally, there exist other limitations in the new claims that are simply not found in any of the cited patents.

The following will discuss the new claims with respect to Larose, Friedman and LeBourgeois in more detail with respect to the present claims.

Larose does not anticipate or suggest the new claims.

The present invention uses the same key (or copies thereof) both to encrypt and decrypt software products¹. For example, in new claim 16 the *single value* is used both to encrypt and decrypt the software product:

¹ Software products are defined in the present invention as executable code, data files, or streaming data.

*'encrypting, at the server computer, the software product by using the single value as the encryption key, and...
decrypting the encrypted software product by using the single value as the decryption key.'*

Also in new claim 16, the *single value* itself is both encrypted and decrypted by using the same key (namely the set of parameters):

*'encrypting, at the server computer, the single value by using members of the first set of parameters as encryption keys, and...
decrypting members of the set of encrypted single values using members of the second set of parameters as decryption keys...'"*

Similar elements are found in the remaining new independent claims that relate to encryption (i.e. new claims 18, 21, 23, 25, and 31). These are uses that define symmetric encryption/decryption keys.

In contrast, Larose is silent on symmetric keys and explicitly requires the use of private-public keys (PPK) "to realize the advantages of" his invention (see Larose Column 7: lines 12-29).

i)...the production of a cryptographic fingerprint..., and ii)protection of that cryptographic fingerprint by encrypting it with a private key that the recipient of the fingerprint may, by using a public key and cryptographic algorithm, verify that the data is intact....These two steps are essential to realize the advantages of the present invention, since without both steps a third party may intervene and alter data without the recipient being able to detect it. (Emphasis added)

The above cited "private" and "public" keys are created from "Public-Private Key (PPK) encryption algorithms" as discussed throughout Larose (e.g., see Larose Column 7: lines 41, Column 7: lines 34 – Column 8: lines 27, Fig. 2 150 "public/Private key pairs," and in Figs. 3a, 3b, and 3c: the "PPK encryption algorithms" 113, "public key" 152, and the "private key" 151).

The aforementioned Larose requirements are the source of many disadvantages, including (for example) the creation and maintenance of PPK pairs, and the sending of an unencrypted public key to the installation computer (e.g. Larose Column 7: lines 12-29, Column 3 lines 46-50, Column 13 lines 39-49). Larose acknowledges the disadvantage of *storing* an unencrypted public key at the installation computer (see Larose Column 13:

lines 59-64), fails to recognize other problems (e.g. the *sending* of unencrypted keys to the installation computer) and in any event does not provide a solution to any of these problems. Therefore, the solution (the present invention) to these unrecognized problems could not have been obvious to Larose.

The present invention both recognizes and overcomes these and other problems² inherent in Larose (and in the other cited patents) by: 1) using symmetric keys that are 2) created from information collected from the installation computer, 3) encrypting software products with such keys, and 4) *attempting to recreate the key each time decryption is necessary*. These methods are disclosed in new claims 23, 31, 33 which do not require the sending of any key to the installation computer, and for those claims that do (new claims 16, 18, 21, 25), such keys are always sent encrypted to the installation computer. Also, rather than storing an unencrypted public key at the installation computer, the present invention recreates the symmetric key when decryption is required³. These limitations (and others) found in the new claim--which provide many advantages over Larose--are simply not found or suggested in Larose.

Therefore, Larose does not anticipate or suggest new claims 16, 18, 21, 23, 25, 31, and 33.

Finally, Larose does not anticipate nor suggest new claim 28--a subject matter entirely absent in Larose--which discloses the authentication of an installation computer (by generating multiple sets of parameters) for purposes of authorizing the downloading, or the resuming of such downloading, of software products.

Larose, combined with Friedman, does not anticipate or suggest the new claims.

Since Larose requires the use of PPK, any other secondary reference that may be joined to Larose must retain that PPK use, or, the secondary reference will be contrary to Larose's teachings. With this in mind, and the above distinguishing of Larose, Larose should be completely removed as a reference.

It then follows that Friedman and/or Lebourgeois cannot be combined with Larose to suggest the present invention as now claimed.

² The present invention also provides many advantages over Larose.

³ See the limitation: "*requesting access to the encrypted software product at the computer, and in response thereto, generating a second set of data from the computer*" found in new claims 21, 23, and 33 and "*generating a second set of parameters*" found in new claims 16, 18, 25, and 31.

Friedman, as primary reference, does not anticipate or suggest the new claims.

Although the Examiner did not consider the Friedman as a *primary* reference, the Applicant will do so now for completeness.

First, the Friedman invention covers an entirely different subject matter than that found in the present invention; for example, Friedman does not disclose protecting software from unauthorized usage. Rather, Friedman relates to interactions between two “security devices” for the purposes of enabling client hosts to then send encrypted messages. It’s important to notice that Friedman’s “client host” is connected to his “security device” as described in Friedman Column 7 lines 59-67 and Fig. 4A, and is analogous to Larose’s ‘installation computer’ and the present invention’s “user’s computer” or “computer” (for simplicity, the ‘client host’ and ‘user’s computer’ or ‘computer’ are all herein referred to as the “installation computer”). It’s also interesting to notice that, as one embodiment, Friedman’s security device is ‘a sealed box which cannot be logged into.’(Friedman Column 9: line 33).

Second, like Larose, Friedman is reliant upon the creation and usage of PPK. The first 2 keys created (of a total of 6) are static and dynamic private keys, both generated when Friedman’s security device is turned on. (Friedman Column 10 lines 21-22 and see Fig. 4a item 400). The static private key, which is not a symmetric key, is the only key created from a “seed” from the security device (as opposed to the client host, see Column 10 lines 27-33 and Fig. 4a security host 400 vs. the client host 404). The dynamic private key is then randomly generated and derived from seeds obtained from seconds, minutes, etc. The static and dynamic public keys are then generated from these private keys from the equation on Column 10 line 63.

Thirdly, when the “client host” *first* sends a message to another network security device: “*a protocol is executed by which the two devices (i) exchange static public keys (unencrypted).*” (Emphasis added). This requirement of exchanging unencrypted public keys is a security problem that the present invention overcomes (see above discussion on Larose).

This required usage of PPK and the subsequent exchange of unencrypted public keys between the security devices, are the enabling basis for all subsequent operations necessary for the Friedman invention (see Friedman Column 11 lines 5-6, also Fig. 8 steps 836, and Column 9 lines 26-28) and (as previously discussed with Larose above) is in direct contrast with the present invention.

Furthermore, Friedman does not generate parameters from the installation computer, nor does Friedman disclose sending such collected information to a sever computer, nor creating a symmetric key from this information, etc. Friedman is also silent on authorizing access to software products, and does not have the limitation of *requesting access to the encrypted software product at the computer, and in response thereto, gen-*

erating a second set of data from the computer as well as other elements found in the present new claims.

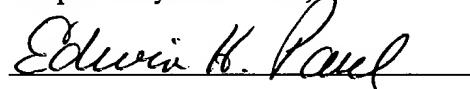
Therefore, Friedman, even as a primary reference, does not anticipate nor suggest new (independent) claims 16, 18, 21, 23, 25, 31 and 33.

Finally, Friedman does not anticipate nor suggest new claim 28-- a subject matter entirely absent in Friedman--which discloses the authentication of an installation computer (by generating multiple sets of parameters) for purposes of authorizing the downloading (or the resuming of such downloading) of software products.

Therefore it is respectfully requested that a notice of allowance be issued for the present invention as now claimed.

Enclosed is a check for \$699.00 that includes a request for a time extension into the third month (\$475.00), five excess independent claims (\$215.00) and one claim beyond twenty (\$9.00). Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,



Edwin H. Paul
Reg. No. 31,405
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500